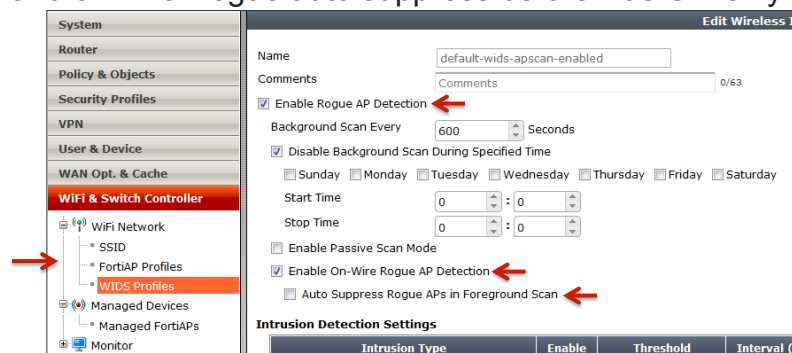




GUI Additions or Enhancements

- Rogue Settings have been moved from AP profile to WIDS profile
- In GUI now BG scan in specific intervals, passive scan and on-wire Rogue auto suppress before was CLI only



GUI additions or enhancements

- VLAN ID can be set in the GUI now for both a bridge and tunnel SSID

The screenshot shows the 'Edit Interface' window for a WiFi SSID. The left sidebar contains the navigation menu with 'WiFi Controller' selected. The main panel shows various configuration options. The 'VLAN ID' field is highlighted with a red oval.

Field	Value
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller
IP/Network Mask	10.11.12.13/255.255.255.0
IPv6 Addressing mode	Manual
IPv6 Address/Prefix	:::0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access
	<input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access
	<input type="checkbox"/> Auto IPsec Request
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access
	<input type="checkbox"/> SSH <input type="checkbox"/> SNMP
DHCP Server	<input type="checkbox"/> Enable
WiFi Settings	
SSID	Testing
Security Mode	WPA2 Personal
Pre-shared Key	***** (8 - 63 characters)
Block Intra-SSID Traffic	<input type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	0

3

FORTINET

New features and enhancements

- Support for 802.11ac access points FAP-221C and FAP-320C

The screenshot shows the 'View All Profiles' window. The table lists various access point profiles. The 'FAP-221C' and 'FAP-320C' entries are highlighted with red boxes.

Name	Platform(s)	Radio 1	Radio 2	Comments	Ref.
11n-only	FWF-20C, FWF-20CA, FWF-30D, ...	2.4GHz 802.11n/g/b			1
FAP11C-default	FAP-11C	2.4GHz 802.11n/g/b			0
FAP14C-default	FAP-14C	2.4GHz 802.11n/g/b			0
FAP28C-default	FAP-28C	2.4GHz 802.11n/g/b			0
FAP112B-default	FAP-112B	2.4GHz 802.11n/g/b			0
FAP210B-default	FAP-210B	2.4GHz 802.11n/g/b			0
FAP220B-default	FAP-220B, FAP-221B	5GHz 802.11n/a	2.4GHz 802.11n/g/b		0
FAP221C-default	FAP-221C	2.4GHz 802.11n/g/b	5GHz 802.11ac/n/a		0
FAP222B-default	FAP-222B	2.4GHz 802.11n/g/b	5GHz 802.11n/a		0
FAP223B-default	FAP-223B	5GHz 802.11n/a	2.4GHz 802.11n/g/b		0
FAP320B-default	FAP-320B	5GHz 802.11n/a	2.4GHz 802.11n/g/b		0
FAP320C-default	FAP-320C	2.4GHz 802.11n/g/b	5GHz 802.11ac/n/a		0

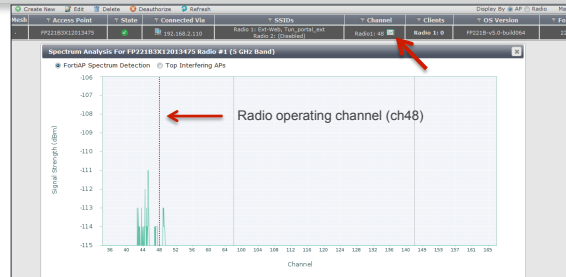
FAP-221C

FAP-320C

4

FORTINET

Spectrum Analysis in certain FAP models



Models with SA

- FAP-221B
- FAP-223B
- FAP-320B

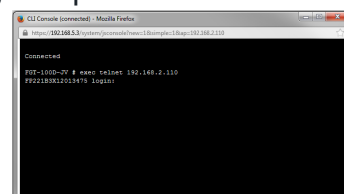
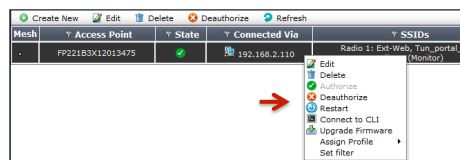
Example using radio in Background Scan

5

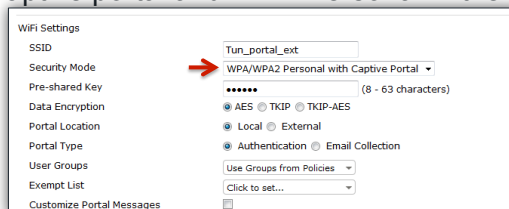
FORTINET

New features and enhancements

- Connect to FAP CLI interface via proxy in FGT. No need for a route to the FAP from managing computer.



- Mixing Captive portal and WPA Personal in the same SSID



6

FORTINET

External Web Captive Portal and Authentication

Edit Interface

Interface Name	Ext-Web-if				
Type	WiFi SSID				
Traffic Mode	Tunnel to Wireless Controller				
IP/Network Mask	10.1.1.1/255.255.255.0				
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FPM-Access <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access				
DHCP Server	<input checked="" type="checkbox"/> Enable				
Address Range	<div> <div>Create New</div> <table border="1"> <thead> <tr> <th>Starting IP</th> <th>End IP</th> </tr> </thead> <tbody> <tr> <td>10.1.1.100</td> <td>10.1.1.254</td> </tr> </tbody> </table> </div>	Starting IP	End IP	10.1.1.100	10.1.1.254
Starting IP	End IP				
10.1.1.100	10.1.1.254				
Netmask	255.255.255.0				
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify				
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify				
Advanced...					
WiFi Settings	<div> <div>SSID</div> <div>Ext-Web</div> </div> <div> <div>Security Mode</div> <div>Captive Portal</div> </div> <div> <div>Portal Location</div> <div><input type="radio"/> Local <input checked="" type="radio"/> External 192.168.5.9/index.php</div> </div> <div> <div>Portal Type</div> <div><input checked="" type="radio"/> Authentication <input type="radio"/> Email Collection</div> </div> <div> <div>User Groups</div> <div>Ext-Web-Auth X</div> <div>Ext-Web-Auth_2 X</div> </div> <div> <div>Exempt List</div> <div>Click to set...</div> </div> <div> <div>Customize Portal Messages</div> <div><input type="checkbox"/></div> </div> <div> <div>Redirect after Authentication (or Disclaimer)</div> <div>http://www.aopa.org</div> </div>				

7

FORTINET

Automatic AP configuration

- Automatic AP configuration disappears and it needs an AP profile now

5.0

Policy

Serial Number: FP22183X12013239

Name: [Empty]

Comments: Write a comment... 0/35

Managed AP Status: Offline

Status: 00:00:00:00:00:00

Base MAC Address: 0

Clients: 0

State: Authorized

Wireless Settings

AP Profile: Automatic (Apply)

☒ Enable WiFi Radio

SSID: ☐ Automatically Inherit all SSIDs ☐ Select SSIDs

Auto TX Power Control: ☒ Disable ☐ Enable

TX Power: [Bar chart]

5.2

Router

Serial Number: FP22183X12013475

Name: [Empty]

Comments: Write a comment... 0/35

Managed AP Status: Online

Status: Connected Via Ethernet (192.168.2.110)

Base MAC Address: 00:09:0F:95:08:48

Join Time: 04/16/14 13:38

Clients: 0

FortiAP OS Version: FP2218-v5.0-build0964 (Upgrade from File)

CLI Console: Connect to CLI

State: Authorized

Wireless Settings

FortiAP Profile: 2218-home ☐ Override Settings

Radio Settings Summary

Radio	Settings	Channels	SSIDs
Radio 1	2218-home	44, 48, 149, 153, 157, 161, 165	[2]
Radio 2	Rogue-AP Scan	-	-

- Option to Override parameters from the AP profile

Override Parameters

FortiAP Profile: 2218-home ☒ Override Settings

☒ Enable WiFi Radio

SSID: ☐ Automatically Inherit all SSIDs ☐ Select SSIDs

Auto TX Power Control: ☒ Disable ☐ Enable

TX Power: [Bar chart]

☐ Do not participate in Rogue AP scanning

Radio Settings Summary

Radio	Settings	Channels	SSIDs
Radio 1	2218-home	44, 48, 149, 153, 157, 161, 165	[2]
Radio 2	Rogue-AP Scan	-	-

8

FORTINET

Split Tunnel in the remote FAPs

The diagram illustrates a FortiAP (FAP) configuration for split tunneling. The FAP is connected to a FortiSwitch Controller. The FAP has two paths: 'To Controller Tunneled' (blue line) and 'To Local Network NATed' (red line).

The screenshot shows the FortiGate configuration interface for the FAP. The left sidebar shows the configuration tree with 'WIFI & Switch Controller' selected. The main panel shows the 'WIFI & Switch Controller' configuration for 'FAP28C-default'. The 'Split Tunneling Subnets(s)' field is set to '172.16.1.0/24'. The 'WIFI Settings' section shows 'Split Tunneling' checked and 'Optional VLAN ID' set to 0. The 'Wireless Settings' section shows 'Enable WiFi Radio' checked and 'SSID' set to '221B-home'.

9

FORTINET

Disable transmission rates

- Disable 802.11b, 802.11bg rates

```
FGT-100D-JV (FAP220B-default) # config radio-2
FGT-100D-JV (radio-2) # set band
802.11b      802.11b radio.
802.11g      802.11g radio.
802.11n      802.11n radio at 2.4G band.
802.11g-only 802.11g only radio.
802.11n-only 802.11n only radio at 2.4G band.
```

Broadcast Suppression

- Broadcast traffic suppression

```
FGT-100D-JV (Ext-Web-if) # set broadcast-suppression
dhcp          Suppress broadcast uplink DHCP messages.
dhcp2         Suppress broadcast downlink DHCP messages.
arp           Suppress broadcast ARP for known wireless clients.
arp2          Suppress broadcast ARP for unknown wireless clients.
netbios-ns    Suppress NetBIOS name services packets with UDP port 137.
netbios-ds    Suppress NetBIOS datagram services packets with UDP port 138.
```

11

FORTINET

Compliance and Certification for some models

- FAP-222B and FAP320C

- » DFS certification

- Proper detection of Radar vs Wireless traffic

- » WFA certification

- Goes beyond the 802.11 standard in order to improve interoperability between vendor devices.

12

FORTINET

